IN THE CLAIMS

1. (Canceled)

2. (Canceled)

3. (Canceled)

4. (Canceled)

5. (Canceled)

6. (Canceled)

7. (Canceled)

8. (Canceled)

9. (Canceled)

10. (Canceled)

11. (Canceled)

12. (Canceled)

13. (Canceled)

14. (Canceled)

15. (Canceled)

16. (Canceled)

17. (Canceled)

18. (Canceled)

19. (Canceled)

20. (Canceled)

21. (Canceled)

22. (Canceled)

23. (Canceled)

24. (Canceled)

25. (Canceled)

26. (Canceled)

27. (Canceled)

28. (Canceled)

29. (Canceled)

30. (Canceled)

31. (Canceled)

32. (Canceled)

33. (Canceled)

34. (Canceled)

35. (Canceled)

36. (Canceled)

37. (Canceled)

38. (Canceled)

39. (Canceled)

40. (Canceled)

41. (Canceled)

42. (Previously presented) A system for securing communications comprising:

an initiating device operable to transmit to a communication server a first request for security of first communications with a first destination device, the initiating device further operable to transmit to the communication server a second request for security of second communications with a second destination device;

the communication server operable to couple to the initiating device and the first destination device, to receive the first request, to select a first algorithm for securing the first communications, to transmit to the initiating device first information identifying the first algorithm, to determine that the first destination device supports encryption of the first communications, and to transmit to the first destination device the first information in response to determining that the first destination device supports encryption of the first communications, the communication server further operable to couple to the second destination device, to receive the second request, to select a second algorithm for securing the second communications, to transmit to the initiating device information identifying the second algorithm, to determine that the second destination device does not support encryption of the second communications, to establish an encrypted link with the initiating device in response to determining that the second destination device does not support encryption of the second communications, and to establish an unencrypted link with the second destination device in response to determining that the second destination device does not support encryption of the second communications;

the first destination device operable to receive the first information, to encrypt a first message for communication to the initiating device using the first algorithm, and to decrypt a second message received by the first destination device using the first algorithm; and

the second destination device operable to transmit a third message to the initiating device through the communication server and to receive a forth message from the initiating device through the communication server.

43. (Previously presented) A system for securing communications comprising:

an initiating device operable to transmit to a communication server a request for security of communications with a destination device;

the communication server operable to couple to the initiating device and the destination device, to receive the request, to select an algorithm for securing the communications, to transmit to the initiating device information identifying the selected algorithm, to determine that the destination device supports encryption of the communications, and to transmit to the destination device the information in response to determining that the destination device supports encryption of the communications; and

the destination device operable to receive the information, to encrypt a first message for communication to the initiating device using the identified algorithm, and to decrypt a second message received by the destination device using the identified algorithm.

44. (Previously presented) The system of Claim 43, wherein:

the initiating device is further operable to decrypt the first message using the identified algorithm and to encrypt the second message using the identified algorithm; and

the initiating device and the destination device are further operable to establish an encrypted communication link for communicating the first message and the second message.

45. (Previously presented) The system of Claim 43, wherein:

the information includes the selected algorithm;

the initiating device is further operable to store the selected algorithm; and

the destination device is further operable to store the selected algorithm.

46. (Previously presented) The system of Claim 43, wherein the request comprises a selection by a user of the initiating device to secure a particular communication session.

47. (Previously presented) The system of Claim 43, wherein the communication server includes a database operable to store a plurality of potential algorithms for use in encrypting the communications.

48. (Previously presented) The system of Claim 43, wherein the initiating device includes:

a user interface operable to receive voice data;

a storage medium operable to store the identified algorithm; and

a communication module operable to couple to the user interface, to couple to the storage medium, and to encrypt the voice data using the identified algorithm for communication to the destination device.

49. (Previously presented) The system of Claim 43, wherein the destination device includes:

a user interface operable to receive voice data;

a storage medium operable to store the identified algorithm; and

a communication module operable to couple to the user interface, to couple to the storage medium, and to encrypt the voice data using the identified algorithm for communication to the initiating device.

50. (Previously presented) A system for securing communications comprising:

an initiating device operable to transmit to a communication server a request for security of communications with a destination device;

the communication server operable to couple to the initiating device and the destination device, to receive the request, to select an algorithm for securing the communications, to transmit to the initiating device information identifying the selected algorithm, to determine that the destination device does not support encryption of the communications, to establish an encrypted link with the initiating device in response to determining that the destination device does not support encryption of the communications, and to establish an unencrypted link with the destination device in response to determining that the destination device does not support encryption of the communications; and

the destination device operable to transmit unencrypted messages to the communication server using the unencrypted link and to receive unencrypted messages from the communication server using the unencrypted link.

51. (Previously presented) The system of Claim 51, wherein:

the initiating device is further operable to receive the information, to encrypt a first message for communication to the destination device through the communication server using the identified algorithm, and to decrypt a second message received from the communication server using the identified algorithm; and

the communication server is further operable to decrypt the first message using the identified algorithm, to transmit the unencrypted first message to the destination device using the unencrypted link, to receive the second message from the destination device, to encrypt the second message using the identified algorithm, and to transmit the encrypted second message to the initiating device using the encrypted link .

52. (Previously presented) The system of Claim 51, wherein:

the information includes the selected algorithm; and

the initiating device is further operable to store the selected algorithm.

53. (Previously presented) The system of Claim 51, wherein the request comprises a selection by a user of the initiating device to secure a particular communication session.

54. (Previously presented) The system of Claim 51, wherein the communication server includes a database operable to store a plurality of potential algorithms for use in encrypting the communications.

55. (Previously presented) The system of Claim 51, wherein the initiating device includes:

a user interface operable to receive voice data;

a storage medium operable to store the identified algorithm; and

a communication module operable to couple to the user interface, to couple to the storage medium, and to encrypt the voice data using the identified algorithm for communication to the communication server.

56. (Previously presented) The system of Claim 51, wherein the destination device includes:

a user interface operable to receive voice data; and

a communication module operable to couple to the user interface and to transmit the voice data to the communication server.

57. (Previously presented) A system for securing communications comprising:

an initiating device operable to transmit a request for encryption of communications with a destination device; and

a communication server operable to receive the request from the initiating device and to determine if the destination device supports encryption of the communications;

wherein, in response to determining that the destination device supports encryption of the communications, the communication server is further operable to facilitate establishment of an encrypted link between the initiating device and the destination device; and

wherein, in response to determining that the destination device does not support encryption of the communications, the communication server is further operable to establish an encrypted link between the initiating device and the communication server and to establish an unencrypted link between the communication server and the destination device.

58. (Previously presented) The system of Claim 57, wherein facilitating establishment of the encrypted link between the initiating device and the destination device includes selecting an algorithm for encrypting the communications and transmitting to the initiating device and the destination device information identifying the selected algorithm.

59. (Previously presented) The system of Claim 58, wherein:

the information includes the selected algorithm; and

the initiating device is further operable to store the selected algorithm.

60. (Previously presented) The system of Claim 57, wherein:

establishing the encrypted link between the initiating device and the communication server includes selecting an algorithm for encrypting the communications and transmitting to the initiating device information identifying the selected algorithm; and

establishing the unencrypted link between the communication server and the destination device includes transmitting an unencrypted message from the communication server to the destination device.

61. (Previously presented) The system of Claim 60, wherein:

the information includes the selected algorithm; and

the initiating device is further operable to store the selected algorithm.

62. (Previously presented) The system of Claim 57, wherein the communication server includes a database operable to store a plurality of algorithms for use in encrypting the communications.

63. (Previously presented) The system of Claim 57, wherein the initiating device includes:

a user interface operable to receive voice data;

a storage medium operable to store a plurality of algorithms for use in encrypting the communications; and

a communication module operable to couple to the user interface, to couple to the storage medium, and to encrypt the voice data using an identified algorithm for communication to the communication server.

64. (Previously presented) The system of Claim 63, wherein the request comprises a selection by a user of the initiating device to secure a particular communication session.

65. (Currently amended) A method for securing communications comprising:

receiving from an initiating device a request for encryption of communications with a destination device;

determining if the destination device supports encryption of the communications;

in response to determining that the destination device supports encryption of the communications, facilitating establishment of an encrypted link between the initiating device and the destination device;

in response to determining that the destination device does not support encryption of the communications:

establishing an encrypted link between the initiating device and ~~the~~ a communication server; and

establishing an unencrypted link between the communication server and the destination device.

66. (Previously presented) The method of Claim 65, wherein facilitating establishment of the encrypted link between the initiating device and the destination device includes:

selecting an algorithm for encrypting the communications; and

transmitting to the initiating device and the destination device information identifying the selected algorithm.

67. (Previously presented) The method of Claim 66, wherein:

the information includes the selected algorithm; and

the initiating device is operable to store the selected algorithm.

68. (Previously presented) The method of Claim 65, wherein:

establishing the encrypted link between the initiating device and the communication server includes:

selecting an algorithm for encrypting the communications; and

transmitting to the initiating device information identifying the selected algorithm; and

establishing the unencrypted link between the communication server and the destination device includes:

transmitting an unencrypted message from the communication server to the destination device.

69. (Previously presented) The method of Claim 68, wherein:

the information includes the selected algorithm; and

the initiating device is operable to store the selected algorithm.

70. (Previously presented) The method of Claim 65, wherein the communication server includes a database operable to store a plurality of algorithms for use in encrypting the communications.

71. (Previously presented) The method of Claim 65, wherein the initiating device includes:

a user interface operable to receive voice data;

a storage medium operable to store a plurality of algorithms for use in encrypting the communications; and

a communication module operable to couple to the user interface, to couple to the storage medium, and to encrypt the voice data using an identified algorithm for communication to the communication server.

72. (Previously presented) The method of Claim 71, wherein the request comprises a selection by a user of the initiating device to secure a particular communication session.

73. (Currently amended) Logic for securing communications comprising, the logic encoded in media and operable when executed to:

receive from an initiating device a request for encryption of communications with a destination device;

determine if the destination device supports encryption of the communications;

in response to determining that the destination device supports encryption of the communications, facilitate establishment of an encrypted link between the initiating device and the destination device;

in response to determining that the destination device does not support encryption of the communications:

establish an encrypted link between the initiating device and ~~the~~ a communication server; and

establish an unencrypted link between the communication server and the destination device.

74. (Previously presented) The logic of Claim 73, wherein facilitating establishment o f the encrypted link between the initiating device and the destination device includes:

selecting an algorithm for encrypting the communications; and

transmitting to the initiating device and the destination device information identifying the selected algorithm.

75. (Previously presented) The logic of Claim 74, wherein:

the information includes the selected algorithm; and

the initiating device is operable to store the selected algorithm.

76. (Previously presented) The logic of Claim 73, wherein:

establishing the encrypted link between the initiating device and the communication server includes:

selecting an algorithm for encrypting the communications; and

transmitting to the initiating device information identifying the selected algorithm; and

establishing the unencrypted link between the communication server and the destination device includes:

transmitting an unencrypted message from the communication server to the destination device.

77. (Previously presented) The logic of Claim 76, wherein:

the information includes the selected algorithm; and

the initiating device is operable to store the selected algorithm.

78. (Previously presented) The logic of Claim 73, wherein the communication server includes a database operable to store a plurality of algorithms for use in encrypting the communications.

79. (Previously presented) The logic of Claim 73, wherein the initiating device includes:

a user interface operable to receive voice data;

a storage medium operable to store a plurality of algorithms for use in encrypting the communications; and

a communication module operable to couple to the user interface, to couple to the storage medium, and to encrypt the voice data using an identified algorithm for communication to the communication server.

80. (Previously presented) The logic of Claim 79, wherein the request comprises a selection by a user of the initiating device to secure a particular communication session.

81. (Currently amended) A system for securing communications comprising:

means for receiving from an initiating device a request for encryption of communications with a destination device;

means for determining if the destination device supports encryption of the communications;

in response to determining that the destination device supports encryption of the communications, means for facilitating establishment of an encrypted link between the initiating device and the destination device;

in response to determining that the destination device does not support encryption of the communications:

means for establishing an encrypted link between the initiating device and ~~the~~ a communication server; and

means for establishing an unencrypted link between the communication server and the destination device.

82. (Previously presented) The system of Claim 81, wherein the means for facilitating establishment of the encrypted link between the initiating device and the destination device includes:

means for selecting an algorithm for encrypting the communications; and

means for transmitting to the initiating device and the destination device information identifying the selected algorithm.